



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,767	03/10/2004	Patrick J. Helland	MS307035.1/MSFTP566US	4181
27195 7590 05/31/2007 AMIN, TUROCY & CALVIN, LLP 24TH FLOOR, NATIONAL CITY CENTER 1900 EAST NINTH STREET CLEVELAND, OH 44114			EXAMINER MORAN, RANDAL D	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 05/31/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/797,767

Applicant(s)

HELLAND ET AL.

Examiner

Randal D. Moran

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 10 March 2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 March 2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 6/1/2004 and 6/4/2004.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. The Information Disclosure Statements filed on 6/1/2004 and 6/4/2004 have been considered by the examiner.
2. Claims 1-27 are pending in the application.
3. Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

### ***Specification***

1. The abstract of the disclosure is objected to because the abstract contains multiple paragraphs.

Art Unit: 2135

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited.

Appropriate correction is required. See MPEP § 608.01(b).

### ***Drawings***

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character **"716"** has been used to designate both **BOB's CERTIFICATE** and **LOGIN BOB**. The specification (p.20- line 17) refers to BOB's CERTIFICATE 720. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 101***

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. **Claim 26** is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, as they do not fall under any of the statutory classes of inventions. The language in the claim raises an issue because the claims are directed to nonfunctional descriptive material (i.e. a compilation or mere arrangement of data), and as such, the claim would be directed to non-statutory subject matter.

A data structure is defined as a physical or logical relationship among data elements, designed to support specific data manipulation functions. As claimed, a data field comprising an encrypted message would not fall under this definition and is therefore non-statutory nonfunctional descriptive material. Arrangements of data without any functional interrelationship is not a process, machine, manufacture or composition of matter. Nonfunctional descriptive material may be claimed in combination with other functional descriptive multi-media material on a computer-readable medium to provide the necessary functional and structural interrelationship to satisfy the requirements of 35 U.S.C. § 101.

***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. **Claim 1-5, 9, 10, and 12-27** are rejected under 35 U.S.C. 102(b) as being anticipated by **Stallings, William. *Cryptography and Network Security; Third Edition*. Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems. Upper Saddle River, NJ. Prentice Hall, 2003. Pgs. 259-265, 290-293, 444, and 655. Hereafter "Stallings".**

3. Considering **Claim 1**, Stallings discloses a message encryption system (p.260- lines 28-36, p. 265- Figure 9.4) comprising: a session key employed to securely exchange a message associated with a dialog (p. 265- lines 18-19); and, an encryption component that employs asymmetric encryption to first securely transmit the session key (p. 292- lines 23-27, p. 293- lines 1-11, Fig. 10.6- (4)), the session key thereafter being employed to encrypt the message and securely exchange the message (p. 444- lines 19-21, p.655- line 21).

Art Unit: 2135

4. Considering **Claim 14**, Stallings discloses a message decryption system (p. 260- lines 25-36, p. 265- Fig. 9.4) comprising: a session key employed to securely exchange a message associated with a dialog (p. 265- lines 18-19); and, a decryption component that employs asymmetric decryption to first securely decrypt the session key (p. 292- lines 23-27, p. 293- lines 1-11), the session key thereafter being employed to decrypt the message (p. 444- lines 19-21, p. 655- lines 21).
5. Considering **Claims 18 and 21**, Stallings discloses a method facilitating session key encryption comprising (p. 444- lines 19-21): firstly encrypting a symmetric session key with a private key (p. 264- lines 18-23); secondly encrypting a result of the first encryption with a public key (p. 264- lines 18-23, p. 265- lines 1-2); and, providing a result of the second encryption as an output (p. 265- Fig. 9.4- item Z).
6. Considering **Claims 22 and 25**, Stallings discloses a method facilitating session key decryption comprising (p. 265- lines 18-19, p. 444- lines 19-21): firstly decrypting a message with a private key (p. 264- lines 18-23, p. 265- lines 1-2); second decrypting a result of the first decryption with a public key (p. 265- Fig. 9.4); and, employing a result of the second decryption as a session key (p. 265- lines 5-19).

7. Considering **Claim 26**, Stallings discloses a data packet transmitted between two or more computer components that facilitates secure distributed communication, the data packet comprising: a data field comprising an encrypted message, the encrypted message first encrypted with a symmetric session (p. 265- Fig. 9.4).
8. Considering **Claim 27**, Stallings discloses a message decryption system (p. 260- lines 25-36, p. 265- Fig. 9.4) comprising: means for receiving an encrypted session key (p. 264- lines 18-23, Fig. 9.4- item Z); means for decrypting the encrypted session key using a private key (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4); means for decrypting a result of the first decryption with a public key (p. 265- Fig. 9.4); means for securely storing a result of the second decryption as a session key (p. 292- lines 23-27, p. 293- lines 1-11, Fig. 10.6- (4)); and, means for employing the session key to decrypt a message (p. p. 444- lines 19-21, p. 655- line 21).
9. Considering **Claim 2**, Stallings discloses the session key comprising a 128-bit randomly generated symmetric key (p. 444- lines 19-30).
10. Considering **Claim 3**, Stallings discloses the encryption component first encrypts the session key employing a private key (p. 264- lines 18-23); the encryption component further encrypts the result of the first encryption employing a public key (p. 264- lines 18-23, p. 265- lines 1-2).



11. Considering **Claims 4 and 19**, Stallings discloses the private key being securely associated with an initiator of the message (p. 265- Fig. 9.4).
12. Considering **Claims 5 and 20**, Stallings discloses the public key being associated with a target of the message (p. 265- Fig. 9.4).
13. Considering **Claim 9**, Stallings discloses the public key being stored as a digital certificate (p. 260- lines 30-32, p. 261- Fig. 9.1- Bob's Public Key Ring).
14. Considering **Claim 10**, Stallings discloses the digital certificate being associated with a user via a login protocol (p. 290, p. 291- lines 1-11).
15. Considering **Claim 12**, Stallings discloses the encryption component further encrypting the message with a private key (p. 444- lines 19-21, p.655- line 21).
16. Considering **Claim 13**, Stallings discloses a broker security system employing the session key of claim 1 (p.260- lines 28-36, p. 265- Figure 9.4).
17. Considering **Claim 15**, Stallings discloses the decryption component first decrypts a message with a private key (p. 264- lines 18-23, p. 265- lines 1-2), the decryption component further decrypting the result of the first decryption with a

Art Unit: 2135

public key (p. 265- Fig. 9.4), the result of the second decryption is the session key (p. 265- lines 5-19).

18. Considering **Claims 16 and 23**, Stallings discloses the private key being securely associated with a target of the message (p. 265- Fig. 9.4).
19. Considering **Claims 17 and 24**, Stallings discloses the public key being associated with an initiator of the message (p. 265- Fig. 9.4).

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. **Claim 11** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings**.

3. Considering **Claim 11**, Stallings discloses the encryption component first encrypts the session key employing a private key (p. 264- lines 18-23), the encryption component further encrypts the result of the first encryption employing

Art Unit: 2135

a public key (p. 264- lines 18-23, p. 265- lines 1-2, p. 265- Fig. 9.4), and, the encryption component separately encrypts the session key with a public key (p. 260- lines 28-28, p. 261- Fig. 9.1), the result of the second encryption and the separate encryption provided as an output (Fig. 9.1, Fig. 9.4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the techniques of the essential elements of public key encryption with the more advanced techniques of confidentiality, secrecy, and authenticity to produce two outputs for the benefit of further increasing the security of the session key transfer (p. 265- lines 5-19).

4. **Claims 6-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings** in view of **VanHeyningen et al. (US 2002/0112152)**, hereafter "VanHeyningen".

5. Considering **Claim 6**, Stallings does not explicitly disclose a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key.

VanHeyningen does explicitly disclose a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective

Art Unit: 2135

subscribers ([0092] lines 1-10, [0139] lines 1-8, Fig. 7B), the trusted agents employing the private key ([0039], [0095]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key as taught by VanHeyningen in order to avoid individually delivering messages to each appropriate recipient device in the network (e.g. point-to-point messaging), as this type of communication restricts the speed and efficiency of the invention (VanHeyningen- [0139] lines 1-8).

6. Considering **Claim 7**, the combination of Stallings and VanHeyningen discloses a trusted agent negotiates a unique session key with a subscriber (VanHeyningen- [0039], [0095]).
7. Considering **Claim 8**, the combination of Stallings and VanHeyningen discloses the trusted agents acting in concert to dynamically load balance distribution for the publisher VanHeyningen ([0091] lines 7-12, Fig. 7B- item 704).

### ***Conclusion***

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 5,299,263 – Yasha split private key.
- US 2004/0133914 – Public-key cryptosystem.
- US 5,557,678 – Centralized central key distribution.
- US 2003/0061493 – Public-key cryptosystem using digital signatures.
- US 5,748,735 – Yasha split private key.
- US 5,960,086 – One time session keys.
- US 7,013,389 – Multicasting.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran, whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran

RDM

5/14/07

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100